UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

SECURITYSCORECARD, INC., Plaintiff, -against- SAFE SECURITIES, INC. d/b/a SAFE SECURITY and MARY POLYAKOVA, Defendants.	Case No. 24-cv-04240 **DECLARATION OF SACHIN BANSAL**

I, Sachin Bansal, declare under penalty of perjury that the following statements are true and correct:

1. I am the President of Plaintiff SecurityScorecard, Inc. ("SSC" or the "Company"), and have personal knowledge of all the facts set forth in this Declaration. I have been employed with the Company since September 2019.

SSC's Business

2. SSC, formed in 2013, is a privately held technology company that has pioneered the cybersecurity risk management field. SSC measures and rates the security of digital infrastructure worldwide and helps organizations and businesses monitor cybersecurity threats around their cloud-based security. It does so, among other things, by utilizing a complex algorithm that takes billions of impressions of the internet daily to find potential vulnerabilities and security holes, generating a cybersecurity score for a business's digital assets.

3. SSC's security ratings allow its customers to identify, understand and manage security risks to their own information systems, as well as the information systems of organizations with whom they work or share data, for example, third-party vendors. SSC offers its security

ratings platform to organizations and businesses globally, including throughout the United States. Over 150 of SSC's active customers are based in the State of New York.

4. SSC's security ratings are sold by "slot." For example, a company seeking to monitor the security vulnerabilities of ten of its third-party supply chain vendors would purchase ten such monitoring slots. By purchasing these slots, customers are given access to SSC's comprehensive ratings database containing continuously updated ratings for millions of companies around the world.

5. SSC also offers complimentary "freemium" access to its security ratings platform, whereby organizations can self-monitor their own ratings score and see high-level security scores of five other organizations, free of charge. Organizations with freemium access cannot see any detailed information about any other organization (which requires the purchase of slots). In many instances, freemium trial customers convert into paying customers once they see the capabilities and benefits of SSC's platform, and its ability to provide insights into other businesses, beyond their own, by purchasing slots.

6. SSC also offers its customers a suite of bespoke professional cybersecurity advisory services, including real-time threat monitoring, digital forensic responses, and third-party cyber risk management.

7. SSC sells its professional cybersecurity advisory services to businesses throughout the United States, including over 150 businesses based in the State of New York.

8. The typical contract value for SSC's security ratings and professional advisory services is in the tens of thousands of dollars per year.

9. Given recent technological advances in artificial intelligence, cybersecurity has become an increasing focus of some of the world's biggest and most profitable companies.

Thousands of companies – including the country's biggest banks, pharmaceutical companies, and insurance companies – already rely upon SSC and its cutting-edge platform and professional services to identify vulnerabilities and prevent online attacks.

10. As cyberterrorism tactics become ever more sophisticated, SSC spends considerable time, energy and resources to stay ahead of the curve, developing innovative counter-techniques and strategies.

11. SSC also spends considerable time, energy and resources identifying prospects and customers. Approximately 85 of SSC's 189 U.S. employees work full time in its Revenue Organization, which is principally comprised of its Business Development Representatives ("BDR") and its Sales Department.

12. SSC's 28-person BDR Department works solely on identifying prospects and generating customer leads. Once a lead is identified, the account is turned over to one of the approximately 35 SSC Sales Directors, who then further identify customer needs, conduct product demonstrations and close customer deals.

13. Since its inception, SSC has spent over $200 million in assembling its full customer and prospect base.

14. SSC's customer and prospect list is the direct result of years of marketing and sales efforts, and cannot be replicated through publicly available sources. The names of SSC's customers and prospects are not readily ascertainable outside the Company.

15. At SSC, customer and prospect information is stored centrally in SSC's Salesforce.com database.

16. SSC undertakes considerable efforts to maintain the secrecy of its trade secrets or confidential or proprietary information (collectively, "Confidential Information"), including the customer and prospect information contained in its Salesforce database.

17. Among other things, SSC's intranet is password protected with multi-factor authentication and role-based permission restrictions. SSC restricts access to information about customers and prospects to those personnel whose access is necessary to their sales, marketing and/or customer servicing activities. All personnel provided such access are subject to confidentiality, non-competition and non-solicitation restrictive covenants. SSC also requires all employees to acknowledge Company policies barring, *inter alia*, emailing confidential documents to their personal email addresses.

18. SSC also provides its employees with Company-issued laptops and mobile phone technology to further protect its Confidential Information.

Polyakova and Her Employment Agreement

19. On February 8, 2020, Mary Polyakova ("Polyakova") was hired by SSC as a Sales Director, with a start date of February 17, 2020. On January 4, 2021, Polyakova was given the title of Regional Sales Director. On June 1, 2022, Polyakova was promoted to Sales Director, Central Region – the title she held until her separation from SSC.

20. Polyakova's February 8, 2020 Offer Letter required that, as an express condition of her employment, she sign the Company's Employment and Proprietary Information and Inventions and Non-Competition Agreement ("SSC Employment Agreement"), and "keep strictly confidential all trade secrets and information that Company holds proprietary or confidential." Attached hereto as **Exhibit 1** is a true and correct copy of Polyakova's February 8, 2020 Offer Letter.

21. Polyakova's February 8, 2020 Offer Letter further provided that Polyakova would receive an annual base salary, and that she would be eligible to participate in a commission plan pursuant to which she would receive the same amount as her base salary if she achieved 100% of the commission plan.

22. It is not unusual in the cybersecurity industry for sales representatives to receive half their pay through these kinds of bonus incentives. It would therefore not be unusual for half of Polyakova's pay at SAFE to be incentive-based, just as it was at SSC.

23. On February 8, 2020, Polyakova signed her SSC Employment Agreement. Attached hereto as **Exhibit 2** is a true and correct copy of Polyakova's SCC Employment Agreement. Among other things, Polyakova agreed to "keep in confidence and trust all Proprietary Information, and [] not directly or indirectly disclose, sell, use, lecture upon or publish any Proprietary Information or anything relating to it without the prior written consent of the Company." Ex. 2 § 1(a).

24. "Proprietary Information" is defined in the SSC Employment Agreement as:

> [I]nformation that has been created, discovered or developed, or has otherwise become known to the Company (including without limitation information created, discovered, developed or made known by or to me during the period of or arising out of my employment by the Company), and/or in which property rights have been assigned or otherwise conveyed to the Company, which information has commercial value in the business in which the Company is engaged," including "(a) inventions, confidential knowledge, trade secrets, ideas, data, programs, works of authorship, know-how, improvements, discoveries, designs, techniques and sensitive information the Company receives from its customers or receives from a third party under obligation to keep confidential; (b) technical information relating to the Company's existing and future products, including, where appropriate and without limitation, manufacturing techniques and procedures, production controls, software, firmware, information, patent disclosures, patent applications, development or experimental work, formulae, engineering or test data, product specification and part lists, names of suppliers, structures, models, techniques, processes and apparatus relating to the same disclosed by the Company to me or obtained by me through observation or examination of information or developments; (c) confidential marketing information (including without limitation

> marketing strategies, customer names and requirements and product and services, prices, margins and costs); (d) confidential future product plans; (e) confidential financial information provided to me by the Company; (f) personnel information (including without limitation employee compensation); and (g) other confidential business information.

Id., Ex. C § 1.4.

25. In the SSC Employment Agreement, Polyakova also expressly "acknowledge[d] and agree[d] that the names, addresses and specifications of the Company's business partners and other associates constitute Proprietary Information and that the sale or unauthorized use or disclosure of this or any other Proprietary Information that [she] obtained during the course of this Agreement would constitute unfair competition with the Company." *See id*. § 4(a).

26. All SSC employees, including Polyakova, are also required to read, accept and follow SSC's Employee Handbook ("Employee Handbook"). Polyakova accepted the terms of the Employee Handbook on November 29, 2022. Attached hereto as **Exhibit 3** is a true and correct copy of the Employee Handbook Polyakova accepted.

27. Under a subheading titled "Communication & Computer Systems," the Employee Handbook provides:

> Employees are prohibited from using personal e-mail accounts or text messaging applications to conduct Company business. Employees may not forward Company emails to a personal email address. Employees may not use any third party email or instant messaging accounts or services (such as GMail, WhatsApp, Yahoo, etc.) for business purposes or any purpose on the Company's computer systems that are not ordinarily used in the performance of their job duties.

Ex. 3 § IV.C.

28. Under a subheading titled "Confidential Information & Conflicts of Interest," the Employee Handbook provides:

> Employees may learn confidential information, including trade secrets, about the Company. Confidential information are items of information relating to the Company, its services, products, clients/customers, suppliers, vendors, and business partners that are not generally known or available to the general public, but have been developed, compiled or

> acquired by the Company at its great effort and expense. Confidential information includes, but is not limited to: business model, methods, operations, strategies, plans for future business, marketing initiatives, products, services, customer information and lists, finances, and revenues. Each employee must safeguard confidential Company information. Confidential information may not be disclosed or distributed to any individual or entity, or used for the benefit of any individual or entity other than the Company, without prior written consent. Employees may not use their position, influence, knowledge of confidential information, including trade secrets, or the Company's assets for personal commercial gain, for the benefit of any competing company or organization, or for the benefit of any other third party except as may be required in performance of their duties as employees of the Company.

Id. § IV.F.

29. All SSC employees, including Polyakova, are also required to read, accept, and follow SSC's "Acceptable Use Policy." Polyakova accepted the terms of SSC's Acceptable Use Policy on October 16, 2023. Attached hereto as **Exhibit 4** is a true and correct copy of SSC's Acceptable Use Policy Polyakova accepted.

30. Among other things, the Acceptable Use Policy provides: "You agree not to use personal email accounts for, but not limited to: Dissemination of confidential information." *Id.* at p. 5.

31. In her role as Sales Director, Polyakova conducted product demonstrations and sold access to SSC's security ratings platform and SSC's professional consulting services. In her role as Sales Director, Polyakova managed four to five sales representatives with accounts across the states and geographical locations documented on the Master East List, as defined below.

32. Although Polyakova worked remotely, she reported to a manager based in New York and managed at least one sales representative based in New York. Therefore, she remotely interacted with SSC personnel in the State of New York on a daily, or near-daily, basis. She participated in new hire training in New York, and she came to New York on at least one other occasion to attend an SSC meeting. Her SSC email signature, which she used regularly to conduct

business and which she used to send to her personal GMail email account the Master East List and CISO Prospect Lists, listed SSC's office address in New York.

33. As a Sales Director, Polyakova had access to SSC's Salesforce database, and to SSC customer work product, customer and prospect proposals, and information about customer current and future needs. Her role with the Company, including her managerial position, necessitated her access to such information.

Safe Securities, Inc.

34. Safe Securities, Inc. *d/b/a* Safe Security ("SAFE") is a direct SSC competitor in the security ratings space and, in particular, the third-party risk management sector. SAFE is a relative newcomer to the industry and far smaller than SSC. Although the cybersecurity industry generally has broad reach, the particular products and services that SSC and SAFE compete to sell have a much narrower scope.

35. In late 2023, SAFE registered for a freemium account on SSC's security ratings platform, which allowed it only to check its own rating and see high-level security scores of five other companies. Like all freemium users, SAFE agreed to SSC's User Agreement, which provided in the preamble:

> You may not access the Services or request information from our Services if you are a direct competitor of SSC, except with our prior written consent. In addition, you may not access the Services for purposes of monitoring their availability, performance or functionality, or for any other competitive purposes.

A true and correct copy of SSC's User Agreement is attached hereto as **Exhibit 5**.

36. SAFE further agreed in the User Agreement that it would never access SSC's platform "in order to build a competitive product or service or use [SSC's cybersecurity ratings and related third-party risk management services] in a way that competes with products or services offered by SSC." *Id*.

37. The User Agreement also expressly states that SSC services, and any proprietary materials provided through the services, constituted SSC confidential information. *Id*.

38. At the time SAFE registered for a freemium account, SSC understood SAFE would access the SSC security ratings platform only to self-monitor its own security score and see limited information about the high-level security scores of five other organizations.

39. SSC has performed all its obligations under the User Agreement by providing limited access to the SSC platform.

SAFE Impermissibly Accesses the SCC Platform for Competitive Purposes

40. On or around May 14, 2024, SSC began investigating whether SSC information was being leaked to SAFE. SSC's in-house information technology professionals gathered forensic information regarding SAFE's activity on SSC's platform, as well as the pre-departure activities of former SSC employees who had joined SAFE.

41. That investigation revealed that SAFE's account on the SSC platform had two active users with the domain name "safe.security": (1) user "anurag.p@safe.security" who first logged in from IP address 182.156.19.250 (the "182 IP Address"), and last logged in on December 22, 2023 from the 182 IP Address; and (2) user "megha.g@safe.security" who last logged in on May 2, 2024 from IP address 49.36.82.71.

42. Based on the information regarding the 182 IP Address, SSC then identified at least three other users who had accessed its platform with that very same IP address: "aamir.ahmad@atlan.com"; "infosec@starlitgroup.net"; and nakul.k@lucideustech.com.

43. The following three additional users also had the same exact user agent – "(Mozilla/5.0 (Macintoch; Intel MacOSX 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/120.0.0.0 Safari/537.36)" – between December 22, 2023 and January 30, 2024: "aamir.ahmad@atlan.com"; "anurag.p@safe.security"; and infosec@starlitgroup.net.

44. The last of those users, infosec@starlitgroup.net, in turn, raised serious red flags for several reasons. SSC authenticated over 400 login records on the site, doing so from various IP addresses, and from various locations, including in India, the United Arab Emirates, and the United States. More importantly, that user appeared to be very actively pulling data from portfolios on the SSC site.

45. The forensic information our team gathered established a high probability that SAFE has been conducting a targeted campaign of setting up account users on SSC's website using a shell or fake company, "Starlit Group," and a fake domain, in order to impermissibly obtain SSC's Confidential Information for competitive purposes. Such information allows SAFE, for example, to check the integrity of its own data and to improve its own offerings by addressing the gaps discovered.

SAFE Improperly Gathers Intel About SSC By Interviewing SSC Employees With No Real Intent of Hiring Them; SSC Sends Cease-and-Desist Letters to SAFE

46. On April 9, 2024, SAFE's Co-Founder and Chief Executive Officer, Saket Modi, bragged to me at a CISO dinner event in Washington, D.C. that SAFE was actively interviewing former SSC employees with no real intention of hiring them, to gather intelligence about SSC's business. As "proof" of the success of those efforts, Mr. Modi disclosed to me confidential statistics on SSC's hiring and restructuring practices that he said SAFE had learned during such interviews. I do not believe that information was publicly available.

47. Fearing a broad misappropriation of our confidential and proprietary information by SAFE, on May 3, 2024, our outside counsel, Pillsbury Winthrop Shaw Pittman LLP ("Pillsbury"), sent a cease-and-desist letter to SAFE. The letter demanded that SAFE immediately

cease its deliberate and unlawful campaign to misappropriate SSC Confidential Information through fake hiring interviews and by tortiously interfering with SSC's former employees' agreements with SSC – notably, the confidentiality and non-competition restrictive covenants contained therein. A true and correct copy of Pillsbury's May 3, 2024 cease-and-desist letter is attached hereto as **Exhibit 6**.

48. On May 7, 2024, SAFE responded, admitting it had "interviewed some candidates who were employed with [SSC]" but claiming its interviews were "in the ordinary course of business" and acts of "fair competition," despite the statements its own Co-Founder and CEO had previously made to me. SAFE also denied possessing or utilizing SSC trade secrets, claiming that any information obtained from newly-hired SSC former employees merely came from their "general experience in the industry." A true and correct copy of SAFE's May 7, 2024 response letter is attached hereto as **Exhibit 7**.

49. That same day, SAFE created a blog post offering "50% OFF current security rating contracts, subscription transfers from SecurityScorecard." A true and correct copy of SAFE's May 7, 2024 blog post is attached hereto as **Exhibit 8**.

50. SAFE also currently devotes an entire page of its website to trying to distinguish its services from SSC's. A true and correct copy of SAFE's webpage titled "Why Customers Choose Safe Over SecurityScorecard" is attached hereto as **Exhibit 9**.

51. After learning that Andrew Peck ("Peck"), another SSC employee, had accepted, or was intending to accept, a position with SAFE, Pillsbury sent a separate cease-and-desist letter to Peck on May 14, 2024, demanding that he, too, comply with his agreement with SSC. A true and correct copy of SSC's May 14, 2024 cease-and-desist letter is attached hereto as **Exhibit 10**.

52. On May 21, 2024, counsel for SAFE responded to the May 14 letter to Peck. SAFE denied any attempt to misappropriate SSC Confidential Information. A true and correct copy of SAFE's May 21, 2024 response letter is attached hereto as **Exhibit 11**.

Polyakova – Now a SAFE Employee – Sends SCC Confidential Information to Her Personal GMail Email Account

53. On or about May 21, 2024, SSC discovered that, on January 4, 2024, Polyakova, while still working at SSC, sent to her personal GMail email account an excel spreadsheet containing detailed confidential and proprietary information about **9,262** SSC customers and active prospects (the "Master East List").

54. This Master East List includes each customer's: annual recurring SSC revenue, projected future annual recurring SSC revenue, contract end dates, SSC licenses purchased and consumed, business alliance partners, activity on SSC's platform, SSC's individual contacts at the customer, and the customer's location (*i.e.*, state or geographical region). Business alliance partners are SSC's strategic partners that enable SSC to reach specific target markets or customers, or bundle SSC services with another company's offering. If a competitor had this information, it could access SSC customers through alliance partners connected to those customers.

55. Polyakova impermissibly sent the Master East List to her personal GMail email account from her SSC email account, "mpolyakova@securityscorecard.io." A true and correct copy of the January 4, 2024 email Polyakova sent to her personal GMail email account, attaching the Master East List is attached hereto as **Exhibit 12**.

56. The Master East List is a compilation of 9,262 records, comprised of over 500 customers, or approximately one-fifth of SSC's entire customer base as of January 4, 2024, and thousands of SSC prospects. The Master East List contains over 1,000 customers and prospects based in the State of New York. *See Id*. Column O.

57. If a competitor were to obtain the Master East List, it would risk the potential destruction of a substantial portion of SSC's core business.

58. Also on or about May 21, 2024, SSC learned that, on March 27 and 28, 2024, Polyakova sent to her personal GMail email account two files containing detailed information about over 200 CISO (Chief Information Security Officer)-level SSC prospects, and the details of the individual contacts at each prospect (the "CISO Prospect Lists"). The information in the CISO Prospect Lists was compiled by SSC as a way to track invites and RSVPs to two business development events: a dinner at Nobu restaurant in Atlanta, Georgia and a dinner at Eddie V's restaurant in Tampa, Florida. Polyakova sent the CISO Prospect Lists to her personal GMail email account from her SSC email account, mpolyakova@securityscorecard.io. Attached hereto as **Exhibits 13** and **14** are true and correct copies of the March 27 and 28, 2024 emails Polyakova sent to her personal GMail email account attaching the CISO Prospect Lists.

59. In total, SSC has expended over $40 million since its inception to develop the information reflected in the Master East List and the CISO Prospect Lists.

60. On April 9, 2024, Polyakova's employment with SSC was terminated.

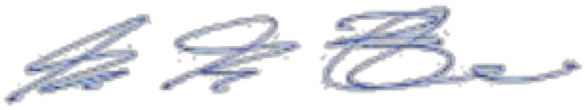
61. On May 24, 2024, a high-paying SSC customer, Veralto Company ("Veralto"), left SSC for SAFE. Veralto is one of the companies on the Master East List stolen by Polyakova.

62. Veralto's contract with SSC was a six-figure contract, with a renewal option.

63. On May 30, 2024, Polyakova posted on LinkedIn, "I am happy to announce that I am starting my new role as VP of Central US at Safe Security." In that post, Polyakova stated she is seeking to hire sales representatives in six of the states specifically covered in the Master East List. Attached hereto as **Exhibit 15** is a true and correct copy of Polyakova's May 30, 2024 LinkedIn post.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Dated: June 3, 2024



Sachin Bansal